

**EXCHANGE MECHANISMS FOR DIGITAL INFORMATION
PACKAGES WITH BANDWIDTH SECURITIZATION,
MULTICHANNEL DIGITAL WATERMARKS, AND KEY MANAGEMENT**

5

RELATED APPLICATIONS

ai7

This application is related to patent applications entitled

"Steganographic Method and Device", Serial No. 08/489,172 filed on June 7,

1995; "Method for Human-Assisted Random Key Generation and Application

10 for Digital Watermark System", Serial No. 08/587,944 filed on January 17,

1996; "Method for Stega-Cipher Protection of Computer Code", Serial No.

08/587,943 filed on January 17, 1996; "Digital Information Commodities

Exchange", Serial No. 08/365,454 filed on December 28, 1994, which is a

continuation of Serial No. 08/083,593 filed on June 30, 1993; and "Optimization

15 Methods For The Insertion, Protection, and Detection of Digital Watermarks In

Digital Data", Serial No. _____, filed on _____.

These related applications are all incorporated herein by reference.

This application is also related to U.S. Patent No. 5,428,606,

"Digital Information Commodities Exchange", issued on June 27, 1995, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

5 ~~The present invention relates to digital watermarks.~~

Digital watermarks exist at a convergence point where creators and publishers of digitized multimedia content demand localized, secured identification and authentication of that content. Because piracy is clearly a disincentive to the digital distribution of copyrighted content, establishment of responsibility for copies and derivative copies of such works is invaluable. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data into the content in such a manner that the content must undergo damage, and therefore a reduction of its value, in order to remove such data for the purpose of subsequent, unauthorized distribution, commercial or otherwise. Legal precedent or attitudinal shifts recognizing the importance of digital watermarks as a necessary component of commercially-distributed content (audio, video, game, etc.) will further the development of acceptable parameters for the exchange of such content by the various parties engaged in such activities. These may include artists, engineers, studios, INTERNET access providers, publishers, agents, on-line service providers, aggregators of content for some form of electronic delivery, on-line retailers, individuals and other related parties that participate in the

transfer of funds or arbitrate the actual delivery of content to intended recipients.

There are a number of hardware and software approaches that attempt to provide protection of multimedia content, including encryption, cryptographic containers, cryptographic envelopes or "cryptolopes", and trusted systems in general. None of these systems places control of copyrights in the hands of the content creator as content is created. Further, none of these systems provide an economically feasible model for the content to be exchanged with its identification embedded within the signals that comprise the content. Given the existence of over 100 million personal computers and many more noncopyright-protected consumer electronic goods (such as audio clips, still pictures and videos), copyrights are most suitably placed within the digitized signals. Playing content is necessary to determine or "establish" its commercial value. Likewise, advertising and broadcast of samples or complete works reinforces demand for the content by making its existence known to market participants (via radio, television, print media or even the INTERNET).

Generally, encryption and cryptographic containers serve copyright holders as a means to protect data in transit between a publisher or distributor and the purchaser of the data. That is, a method of securing the delivery of copyrighted material from one location to another is performed by using variations of public key cryptography or other cryptosystems. Cryptolopes are

suited specifically for copyrighted text that is time sensitive, such as newspapers, where intellectual property rights and origin are made a permanent part of the file.

The basis for public key cryptography is provided, for example, in a number of patented inventions. Information on public-key cryptosystems can be obtained from U.S. Patent No. 4,200,770 to Hellman et al., U.S. Patent No. 4,218,582 to Hellman et al., U.S. Patent No. 4,405,829 to Riverst et al., and U.S. Patent No. 4,424,414 to Hellman et al. Digitally-sampled copyrighted material is a special case because of its long term value coupled with the ease and perfection in creating copies and transmitting by general purpose computing and telecommunications devices. In this special case of digitally-sampled material, there is no loss of quality in derivative works and no identifiable differences between one copy and any other subsequent copy.

For creators of content, distribution costs may be minimized with electronic transmission of copyrighted works. Unfortunately, seeking some form of informational or commercial return via electronic exchange is ill-advised, absent the establishment of responsibility of specific copies or instances of copies or some form of trusted system in general.

20 SUMMARY OF THE INVENTION

INS 93 937 The present invention allows the establishing of responsibility of specific copies or instances of copies using digital watermarks.

The present invention relates to methods for the management and distribution of digital watermark keys (e.g., private, semiprivate and public) and the extension of information associated with such keys in order to create a mechanism for the securitization of multimedia titles to which the keys apply.

5 The present invention additionally relates to "distributed" keys to better define rights that are traded between transacting parties in exchanging information or content.

10 The present invention additionally provides improvements in using digital watermark information. For example, the speed of performing a key search for watermarks within content is increased. Additionally, more than one party can cooperate in adding distinguished watermarks at various stages of distribution without destroying watermarks previously placed in the content.

15 Digital watermarks make possible more objective commercial exchanges of content. Trusted systems are more costly but achieve the same goal by establishing the identity of all electronic exchange participants. Digital watermark per copy systems, however, are not on a simple level of establishing responsibility of a master work and its derivative copy only.

20 Multichannel watermarks with private, semiprivate and public keys used as different levels of neighboring rights assist in the creation of a self-contained model for the exchange of copyrighted works. Private key watermarks can be inserted into content to establish ownership rights (copyright, master right, etc.) with the content creator or an agent of the content creator maintaining control

over the key. Semiprivate watermark keys can exist in a separate channel of the information signals that make up the work to be exchanged for subsequently delegating responsibility to distributors or sales entities to restrict resale rights in the same manner that physical goods have an exchange of title corresponding to their sale. And finally, public watermark keys exist as an independent component of the identification, authentication or advertising of a given work to be widely distributed over networks for initiating the purchase of a sought-after work. The market will still rely upon trusted parties who report any distribution or exchange of derivative watermarked copies of these "protected" works. Recognition of copyrights as well as the desire to prevent piracy is a fundamental motive of enforcement which uses the mechanism of digital watermarks to alleviate fears of copyright holders and transacting parties that responsibility and payment for copyrights cannot be established and accomplished.

A necessity has arisen for a system that better defines methods for recognizing these rights and, with the further creation of bandwidth rights, as in the present invention, makes possible a distributed model for digital distribution of content which combines the security of a digital watermark system with efficient barter mechanisms for handling the actual delivery of digital goods.

The present invention relates to methods for the management and distribution of digital watermark keys (e.g., private, semiprivate and public) and the extension of information associated with such keys in order to create a

mechanism for the securitization of multimedia titles to which the keys apply.

To differentiate the present invention from public key cryptography, use of

"private ", "semiprivate", and "public" keys herein refers to the use of such

"information" with the stated purpose of distributing goods and watermarking

5 content, not encryption or cryptography in the general sense.

The present invention additionally relates to "distributed" keys to better define rights that are traded between transacting parties in exchanging

information or content. Such keys can carry additional pricing and timing

information, and represent coupons, warrants or similar financial instruments

10 for purchase of copies of the corresponding title at particular prices within a

specified period of time. These instruments, as extended keys, can be

collected on servers, distributed to individuals and redeemed as part of a

transaction to purchase the content. The basis for this type of content trading

system is described in U.S. Patent No. 5,428,606 entitled "Digital Information

15 Commodities Exchange" (hereinafter, also referred to as "the DICE patent").

The present invention improves on the invention described in the DICE patent

by integrating into the DICE exchange (i.e., The Digital Information

Commodities Exchange) the copyright protection mechanism of digital

watermarks. Digital watermarks are described in the following patent

20 applications assigned to The DICE Company: "Steganographic Method and

Device", Serial No. 08/489,172; "Method for Stega-Cipher Protection of

Computer Code", Serial No. 08/587,943; "Method for Human Assisted

Random Key Generation and Application for Digital Watermark System", Serial No. 08/587,944; and "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data", Serial No. _____.

In addition, the present invention improves upon the techniques of
5 digital watermark systems, described in the patent applications listed above, by adding methods for the use of this information which allow for improvements in the speed of performing a key search for watermarks within content, and by allowing for more than one party to cooperate in adding distinguished watermarks at various stages of distribution without destroying watermarks
10 previously placed in the content. At the same time, these methods minimize the amount of information which any one party must divulge to another party, and prevent "downstream" parties from compromising or otherwise gaining control of watermarks embedded by "upstream" parties.

Further improvements of the present invention include the incorporation
15 of retail models using well-known commodities exchanges to accomplish more efficient means of advertising, negotiating, and delivering digital goods in an anonymous marketplace as commonly characterized by such systems as the INTERNET. Video-on-demand models, quality of service reservations considered in subscriber models, and related models that have been referred
20 to as "time shares" for parceling up processing time in a general computing network will also be differentiated.

DETAILED DESCRIPTION

a47

There are several issues preventing greater volumes of electronic distribution of multimedia content. While such distribution is in fact technically feasible at the present time, attempts at commercially-viable systems are still

5 plagued by these problems, and render digital multimedia exchanges unsatisfactory on a scale comparable to mass retailing in consumer goods markets, such as that of digital audio recordings on compact discs (CDs). While it is possible to transmit a single copy of a digital recording, as 16-bit 44.1 kHz stereo (CD-quality), to an individual from an archive, making such

10 copies available to a large number of paying consumers on demand is still not yet being implemented. The problems fall into several classes, including distribution bandwidth, copyright protection, technological complexities, and "efficient shopping."

In a similar vein to distribution of physical goods in the real world,

15 bandwidth and developments that effectively increase bandwidth are creating profound new business models in how content creators and publishers can distribute their works. From the simplest compression schemes, to actual use of "wired" technology including ISDN, cable modems, ATM and fiber optic lines, the trend is moving toward greater amounts of bandwidth available to

20 on-line users. It is a conundrum of the digital age that the object of bandwidth use will most likely require downloads of copyrighted works, or transaction-based models, to justify such increases in bandwidth availability.

Ins a4

004040:6954360

content, music or otherwise, and the durability of the medium itself, which can be played without loss of quality far more times than any analog tape.

However, the CD is a storage media that must be manufactured, put into inventory, sent by carrier to physical locations, etc., and has an inherent

5 tendency to standardization (the CD is actually a specification determined by manufacturers of both the hardware and software).

Hard costs for marketing and promotion may be better spent across a larger geographical segment, easily accomplished by such electronic networks as the INTERNET but harder to assess in terms of actual sales. Determining
10 market reception is also difficult when buyers are relatively unknown and not available for localized comment or analysis in typical, physical retail store sites (such as Tower Records, Sam Goody's, Blockbuster, etc.).

What equalizes physical mediums such as DAT, CD and DVD, are the lines running between geographic locations, including POTs (i.e., Plain Old
15 Telephone), cable, fiber optic, electric power lines and wireless access points including radio, satellite, cellular phones, and the like. The digitization of these access points and the networks that make them possible ultimately dictate what devices will be appropriate to consumers of the present day and the future. That is, matters of cost and even reputation will increasingly dictate the
20 economics of the distribution of digital content, much the way matters of costs and reputation dictate sales in other consumer goods markets. No longer will it necessarily be important to manufacture X number of copies of a given work

for distribution at N number of sites to capture the optimal market of consumers. The present invention is predicated on not only the existence of a plurality of access points, as discussed in the DICE patent (U.S. Patent No. 5,428,606), but also on a domain where digital content can pass freely

5 between networks much as the INTERNET works with a common protocol (TCP/IP) to facilitate the exchange of data files. However, the ability and desire to orient delivery of digitized content around the specs that describe the content, rather than protocols necessary to redefine the content for exchange over a specific protocol (such as TCP/IP), can better define more convenient

10 delivery of the content between publishers and subscribers given the heterogeneous nature of transmission media (POTs, cable, etc.), the unchanging behavior of "consumer electronically-described" media content (FM-quality, CD-quality, etc.), and the varying configurations of pipes utilized by both publishers and subscribers more concerned with the distribution and

15 exchange of digital goods, not configurations of the immediate input and output devices that are linked by a multitude of electronic exchanges (cable, POTs, wireless, electric power, etc.). Indeed, shifting only the recordable media cost to consumers that, for the most part, already own one or more such devices and may have exposure to a number of broadcast and advertising media

20 (INTERNET, on-line services, radio, cable, print, etc.) may afford both buyers and sellers the cheapest means of profitably exchanging digital goods.

At present, over 15% of the U.S. population has more than one phone

line, 60 million households have cable television, and 15 million consumers are on-line subscribers. ISDN is also experiencing growing demand in the U.S. to give consumers higher bandwidth in the interim. Projected increases of bandwidth portend future supply and demand of larger data files of copyrighted

5 passive works (e.g., music, pictures, video, etc.) and interactive works (e.g., games, software, etc.), thus putting pressure on the need for increases of bandwidth. Never before has increased available bandwidth suffered from a lack of demand by users. In other words, new bandwidth seems to create its own demand. Much of the presumption in increased investments in creating

10 the bandwidth has been to enable the transfer of audio, video, and multimedia files that typically occupy more than 5 MB of space per file. The misanalyzed aspect of these investment plans is a method for addressing digital piracy of copyrighted works and efficient, market-based allocation of the subsequent bandwidth by users. The present invention better defines maximized

15 operations dependent more on the specs that describe playback of content than redefining additional protocols which add additional and unnecessary levels to the playback of the content. With such advances, exchanging media content can potentially be made as easy as exchanging physical content.

The present invention additionally reduces costs in the distribution

20 process, provides the monitoring of, and thus ability to protect, copyrights within the media, and allows the implementation of better payment systems suited to the distribution of digital goods. What is clear is that bandwidth may

never be unlimited, but with consideration made to real world economics, efficient and realistic methods for considering "fill rate" (the actual titles "delivered" to a purchaser versus the titles "ordered"), speed (actual time it takes for a consumer to receive desired content), and cost (expense given

5 trade-offs of immediate availability at a given price point to the consumer, e.g., immediate fulfilment equates to higher pricing, versus delayed delivery of the same content at a lower price) all represent input variables in a real world "retail experience" that may be replicated in the digital domain. The present invention takes into consideration the behavior of parties engaged in selling

10 content that may not be initially valued at the same price by all market participants and is subject to the same promotion hype as goods in the real world. In the digital domain, sampling, trailers, and pre-release hype can be replicated to foster demand for a given title of a digital good with many of the same results that are experienced in the real world.

15 Evidence of supposedly more efficient schemes for retail include U.S. Patent No. 4,528,643 to Freeny, which shifts much of the manufacturing costs to physical retail sites, thus increasing the cost of doing business on the retail side with possible increases of convenience to the consumer. In the Freeny patent, retailers are envisioned to have localized reproduction of given digitized

20 products (music, video, etc.) and a means to use "owner authorization codes" to verify the electronic transmission of a given work from some "master file unit" to recordable media (VCR, recordable CD, etc.). Freeny refers to mail order

clubs and other direct marketing efforts as being inefficient versus the localized manufacturing structure. These predictions have since been proven false. It is because of the nebulous concept of intellectual property coupled with the extreme expense on retailers for the in-store manufacturing units that makes clear the benefit of leveraging available bandwidth to content creators, publishers, consumers and "pipe owners." The efficiency of such operations as Federal Express in delivering even small packages in under 24 hours and the ability of "fulfilment houses" to effectively carry all but the most obscure titles (music, books, videos, etc.) has made actual "manufacturing" of a given physical media object (CD, VHS tape, etc.) or what Freeny describes as a "material object" simply uneconomical and increasingly irrelevant in an age when bandwidth and digital recording devices such as PCs, Minidiscs, digital video disks (DVD), etc. make physical retail-based, or in-store, copying more of an inconvenience.

The paradox of digital copies is the ease and relatively inexpensive operation of making perfect copies from a single instance of a work, thus providing the potential of unauthorized copies or piracy. The binary data that comprises a digitized work is an approximation of an analog signal. As is well known binary ones and zeros can be manipulated to form words, audio, pictures, video, etc. Manners in which individual copies can be marked so that responsibility can be assigned to individual copies that are derivatives of the master copy is documented in the patent applications by The DICE Company

referenced above (i.e., U.S. Patent No. 5,428,606, and the "Steganographicc
Method and Device", "Method for Human-Assisted Random Key Generation
and Application for Digital Watermark System", "Method for Stega-Cipher
Protection of Computer Code", "Digital Information Commodities Exchange"
5 and "Optimization Methods for the Insertion, Protection, and Detection of
Digital Watermarks In Digital Data" applications), and in alternative proposals
by Digimarc Corporation (a form of pseudo-randomly encoding digital
signatures into images), Bolt Beranek & Newman (Preuss et al. patent, U.S.
Patent No. 5,319,735) (embedded signaling) and others. Additional proposals
10 for cryptolopes and cryptographic containers by IBM and Electronic Publishing
Resources (EPR) place control of copyrights and other "rights" in the control of
IBM and EPR, not the individual content creator or publisher. IBM and EPR
are creating a form of "trusted systems." What is clear is that trusted systems,
where all parties are known in some way to establish responsibility for
15 instances of copied files, are not realistically possible with the number and
ease of manufacture of digitization systems such as general purpose
computing devices. At present, over 100 million such devices are in existence,
and it is not possible to guarantee that all of these systems will be made to
adhere to the defined parameters of a trusted machine for verification and the
20 establishment of responsibility for individual copies made of digital works.
Profit motives continue to exist for individuals to make perfect copies and
distribute these copies without paying the parties responsible for creating and

007049-990466
0543539-040700

distributing the content. Moreover, beyond considerations of digital exchanges that do establish responsibility for the goods being sought, the digital bits that comprise the commercially-valuable works suffer both from lack of use by parties seeking more secured means of distributing and marking content, and

5 legal tanglings by parties that own the copyrights and seek any entity deemed to copy works illicitly for settlement of disputes. That is, with the great number of untrusted systems in existence, many copyright holders have resorted to legal challenges of on-line services and individuals found to be in possession of unauthorized copies of copyrighted works. The resultant digital marketplace

10 tends to favor larger companies who can afford to seek legal settlements without delivering any substantial benefit over smaller companies that for many reasons would otherwise favor digital distribution of content to minimize overall costs. The remedy for such problems is addressed in the previously discussed related U.S. patent and patent applications by The DICE Company

15 and other parties mentioned above (e.g., NEC, Digimarc, EPR, IBM, etc.)

The present invention relates to methods for parceling rights to benefit buyers and sellers of digital works in ways that even the playing field of the marketplace given the resource of electronic marketplaces that can work with such networks as the INTERNET. Too often physical world solutions are

20 offered where digital domain considerations are completely ignored.

Another issue relating to the present invention involves haphazard grafting of physical world pricing and automated payment systems onto digital

systems. Issues of inventory, physical movement, and manufacture of goods are completely muted in digital exchanges, but are replaced by bandwidth utilization and efficiency, one-to-one connections, and one-to-many connections, i.e., seeking and reaching customers in an anonymous marketplace. It is these issues that will better determine the price of a given digital good. Timing of the good (that is, live versus broadcast rerelease of the same digital good) and the necessity of filters or brokers which guide individuals to acceptable goods are variables that will play roles in determining the ultimate efficiency of exchanging digital goods.

10 Among some of the proposed systems are a proposal by Wave Systems, which necessitates the use of proprietary boxes using encryption to tie the user's "exchange device " to some party that can determine the validity of the box, a trusted system. Unfortunately, adoption of such a solution would necessitate the purchase of separate boxes for separate vendors of particular works or the routing of all digital goods through a proprietary system that then resembles closed cable, video-on-demand, and private networks. Similar approaches are used by merchants using credit card processors and the use of credit card authorization devices and paying incremental costs for the use and security delivered by the credit card processor. Further systems include

15 log-in procedures to validate the accessing party's identification. The premium paid for such systems is arguably excessive when compared to content creator-controlled implementation of digital watermarks and an exchange by

which all distribution parties are engaged in the marketplace to pay for bandwidth rights to market-test given digital goods. The only alternative available to smaller content creators and artists is to sell content at no charge, thus jeopardizing potential future returns, or purchasing outright the hardware to plug-in to existing networks, an excessive cost if such "bandwidth" could be more fairly-priced in a need-based system such as that discussed in this disclosure.

As an improvement to the system discussed in U.S. Patent No. 5,428,606, the present invention ties so-called "header" files into the actual content. U.S. Patent No. 5,428,606 addresses the separation of content from its references ("header") to facilitate more efficient access and exchange of digital content. The "headers" described in this patent might be construed in the real world as options or futures, and is discussed below. The present invention concerns itself with creating a method for introducing a layer of price and distribution determination given the necessity of payment in delivering digital content between points in the digital domain which may not suffer from any physical limitations but are limited by bandwidth considerations.

Some attempts at the exchange of content are being tried with existing networks such as the INTERNET. The complexities extant are apparent in the requirements of the operating protocols and the dependence of TCP/IP for orienting content and subsequently playing it back through "players" that are TCP/IP compliant, if the INTERNET is solely considered. More issues

regarding the INTERNET are further discussed below.

Conceptually, "agents" partially meet some of the expectations of a content-based system, except agents are also dependent on participation by sites willing to allow for pure price comparisons and later reporting to the purchasing party. At present, many sites lock out such agents as they seek to profit by value-added services which are not considered by an agent when "shopping prices." Video-on-demand systems also propose a more closed system that is reliant on a proprietary network to deliver a video (or audio for that matter) to a consumer with the least amount of time delay while satisfying the demands for the video by many other consumers seeking the same video at the same time. The difference between such a system and that disclosed in the present invention is that such video-on-demand networks propose "subscriber" models where all consumers are deemed to have the same right to a given, demanded, piece of content at any time. That is, all participants are "subscribers" who prepay a fee structure that cannot necessarily be justified given bandwidth and processing limitations for delivering digital goods "on demand." In such a system, infrastructure cost can run as high as 5,000 dollars per subscriber, as with Time Warner's system in Orlando, Florida.

In the present invention, time is not an absolute standard to measure satisfaction. In the same manner that retail stores cannot always have a given audio or video work "on demand," other factors may play into the competitiveness of that entity to contribute to the satisfaction of a given

002040:0004550

consumer. These issues include a depth (number of copies or copyrights of a given title) or breadth (number) of titles offered, a variety of delivery mediums to satisfy customers with varying access infrastructure (cable, telephone, fiber optic, electric power, etc.), pricing, and, finally, service as it can be applied in

5 an anonymous marketplace. Services may include the know-how of buyers employed by a given digital broker in offering samples of new releases or unknown artists, as well as special price offers given the amount and types of digital goods being purchased. What is certain is that a "subscriber" model is subject to the same deficiencies of a cable model or proprietary on-line service

10 that may not be able to balance financial considerations with the variety and cost of titles sought by individuals at any given time. On the seller side, maximizing profit per title cannot always be satisfied if distribution control or proprietary rights are granted to any single entity which, by the present nature of the INTERNET and future interpretations of on-line commerce, cannot be

15 guaranteed. Indeed, the above-mentioned U.S. Patent No. 5,428,606 discusses a situation where all subscribers can be publishers. For smaller parties, naturally lacking sufficient resources to initially and adequately market and promote titles, a more open system for negotiating distribution rights must be sought by commoditizing the good that most effects exchange of their

20 goods in the digital domain (i.e., bandwidth).

Moreover, in an anonymous marketplace, even small aggregators of content may be able to adequately promote the digital properties of other small

content creators with value-added services. These services, such as samples of content, used to entice buyers, just as trailers create demand for upcoming movies, could be delivered to a differing type of subscriber, much as the music aficionados who subscribe to College Music Journal (CMJ) and other
5 resources to sample new, relatively uncommercial music. Samples of 10-30 seconds could be sent directly to consumer e-mail addresses replicating the prevalent listening bars set up by physical music retailers seeking to introduce new titles to eager listeners. Other services might be more representative of "music chat rooms" or special title web-sites, to more fully entice potential
10 buyers with a greater amount of purchase information. Much of the premise of such services and fulfilling demand for content, however, will require a more efficient means to allocate bandwidth according to an embodiment of the present invention. Without such bandwidth allocation, even small digital goods vendors will need to purchase substantial hardware, from T1 lines to high-
15 powered UNIX machines, meaning high entry or fixed costs, to effectively market what may only be a single title in a year.

The present invention deals with commoditization of the digital distribution of multimedia content. It is important to note that in creating such a market, one must consider two commodities. One is the title, or data itself, of
20 which there is a theoretical unlimited supply over time (limited only by how many copies of a given title that can be made). The second commodity is bandwidth. This is a commodity which must be treated more like traditional

commodities, since its supply is physically limited over discrete periods of time

"Fatter" pipes and compression can only increase upper limits given the

observed tendency for larger data files to accompany bandwidth increases in

the short term. In practice, bandwidth limits act as a parameter on the capacity

5 of a distribution channel at any given moment in time, since there is a fixed

amount of bandwidth. In dealing with commercial markets, where, for example,

80% of the consumers want 20% of the products, (and for digital marketplaces,

generally all at the same instant), some premium can be observed as with "first

come first serve" principles in physical sales channels. The difference is that

10 an additional copy of a digital work can be made almost instantaneously,

although additional bandwidth cannot be replicated. Even in instances with

theoretically infinite time to fill all orders, most buyers will have given up and

"left" the exchange after waiting a short period, during which time they get no

satisfaction, measured explicitly by an access or download of a specifically

15 desired title. On-line services today are typically plagued by this shortfall,

leading most users to complaints of access and speed. Market-based

principles could alleviate some of this problem on both the buyer and seller

side if bandwidth is treated as the commodity it is. "Quality-of-service"

proposals partially address this issue, though costs are stacked on the seller

20 side because such systems are almost always proprietary given the

requirement of high infrastructure expenses to enable timely delivery to all

subscribers to the "private" network.

002040-6554560

The present invention combines "efficient shopping" principles with the commoditization of bandwidth and titles to create an exchange, under principles as described in the DICE patent, where in place of a security, one can buy titles where a component of the title price is actually a bandwidth option, or bandwidth right. The purchaser buys a right on the underlying title to take delivery of the title via a particular transport medium which uses a particular allocation of transmission bandwidth at a particular time. According to an additional embodiment of the present invention, distributor or content aggregator-only purchases of bandwidth are stipulated as options for digital distribution increase, in terms of available channels (such as cable, satellite, etc.). In this case, the end user never deals with the bandwidth right, although the costs of such rights may be passed on in the retail price of the title which is purchased and downloaded. In other words, the distributor must purchase rights in advance to support a projected volume level of distribution. These pre-purchased rights are then attached to individual downloads. These instruments can vary in price, much like stock options, based on time. Only, in this case, it is the amount of time required to receive the underlying security, which implicitly indicates how much bandwidth will be used by the buyer. The bandwidth actually implies time. The spectrum could range from lowest bandwidth, such as an e-mail delivery by POTs lines, which uses bandwidth when it is otherwise not in use and is at the convenience of the seller (sender), and not the buyer (receiver), to highest bandwidth that may be parallel or direct

access fiber optic line which may be necessary for users acting as wholesalers between electronically -linked parties who seek content for negotiated delivery.

U.S. Patent No. 5,428,606 uses the concept of a "DIP" ("digital information packet") header to create an advertising, distribution, and pricing
5 device which allows for the dissemination of references to and description of particular titles available electronically. The DICE Company's related digital watermark patent and patent applications as discussed previously disclose an exchange model for digitally-watermarked content and digital watermark keys whereby keys which allow a party to scan or imprint watermarks are
10 distributed, possibly electronically, at the discretion of the controlling party. Both these methods have in common the fact that they allow for the distribution of some information related to an underlying work, without distributing the work itself. It is in the interest of simplicity, therefore, to allow for the combination or conjunction of these information items in addition to associating them with a
15 bandwidth right or option for the downloading of the copyrighted work.

Essentially, some of this negotiation of bandwidth takes place between the "Baby Bells" and AT&T or other long distance providers when settling rights-of-way between points of a telephone conversation. At present, a key difference is that the utility value of a phone call sets the value of the "phone
20 time" being sold. Bandwidth rights as envisioned in an embodiment of the present invention price the commodity of bandwidth given the luxury item being sought (i.e., data or content). The present invention seeks to value the

immediacy as well as convenience (of which price may play a role) in receiving a given packet of data (media content, software, etc.) from one or many locations where it may be available to other locations. The lines may be heterogeneous between points, thus offering a more open bidding system

5 between line owners, content creators and publishers, and end users or consumers. At present, no such "negotiation" can be handled by network operators running lines to the same home or office. Indeed, lines are usually charged at a fixed fee, not by what amount they are used. In some cases, lines are billed by a raw measure of the data transferred, but not in relation to

10 the actual value of such data nor with respect to the value of other transfers which might occur simultaneously via the same line. This sort of billing-by-byte tends to discourage use, but it is a very coarse tool with which to manage utilization. To fill the middle market for demand of these lines for telecommunications lines in particular, long distance carriers such as AT&T,

15 MCI and Sprint sell excess capacity to "wholesalers," while the larger companies generally have price constraints.

The potential demand for bandwidth is clearly evident with such widespread use of networks, epitomized by the INTERNET. But, as previously discussed, smaller, specialist "retailers" and "wholesalers" of services or

20 content that could be marketed over these lines are not efficient. The potential for efficient pricing exists as demonstrated by "call-back" services, which route calls from one location through a third party location, benefitting from that

location's line pricing, though the overall market for such services is still only about \$300 million annually. What restricts more open allocation of bandwidth is political in nature. At the same time, cross subsidization of local phone access from more expensive long distance and international service is open for

5 rationalization envisioned by the present invention. Even if more network services could offer greater returns for line use, and thus bandwidth use, public telephony accounts for over 85% of the market. A particular model being evaluated is called "sender takes all" where the access point, or the party that provides access to an end user, would take all the access charges. This is

10 similar to the INTERNET, but is still stacked against smaller players, of which content providers are the least favored if they seek "distribution channels" over networks that still lack proper market incentives for use of bandwidth. Some other models being considered include a single access charge, which is an improvement over current international accounting standards being negotiated

15 between countries. Still, this model does not take into consideration the available bandwidth controlled by non-telecommunications parties, such as cable companies, though ultimately the commodity being brokered is actually common bandwidth. The uneasy balance in negotiating access is being tempered by the steady increase by telecommunications companies to

20 upgrade their lines to offer comparable bandwidth access as that presently available through cable companies. A final issue for consideration is the mobile market of cellular phones and other similar technologies though there

are far more restrictions on the amount of available bandwidth for content distribution, the move to free up more radio spectrum for digital signals may lead to increases as high as a hundredfold in the capacity of the network which would make the electronic delivery of a single audio track realistic. Still, the present invention seeks the imposition of market-based pricing of available bandwidth to end users and content providers given the absence of any such system currently.

With the recent removal of barriers which previously prevented competition between cable companies, telecommunications companies, and regional Bell operating companies (RBOCs) the matter of cost of services or content being delivered over common pipes and the concept of a single entity dominating the "network" will almost surely come to an end as many companies are strongly positioned in their local markets. At present, "local loop" access to end users still presents formidable barriers to competition-- 40-45% of the cost of a long distance call is paid to the RBOC whose lines run into the home or business making the call. In total, the cost to a network for local distribution is approximately 80%. Proposals for separating a network into its infrastructure and service components would likely benefit from the invention being outlined. In such a scenario, the owner of the network would offer access to providers on the same terms, while managing the operation of the infrastructure. Simple models, such as flat rate INTERNET access, are problematic in the overall model for market-based pricing of bandwidth in that

capital costs are completely ignored though such costs are the parameter by which any business model must be judged. Though the cost of an extra phone call over a given network may be negligible, the cost of pumping large multimedia files, which have far different utility value to users of the network

5 versus a "telephone conversation," is relatively high in the aggregate and can be witnessed with the progressively slow performance of many on-line providers and the INTERNET. The goal for network providers will be to offer value-added services to users as well as value-added access to content that is controlled by copyright holders seeking maximum distribution (given speed and

10 quality) to content seekers. These parties may only need the network at certain times or for certain releases of content. Meanwhile, periphery services such as music sampling, game testing, beta software distribution, will most likely comprise value-added services beyond the present scope of strict telephony. The pressure, generated from capital cost concerns, to provide a system that

15 prices speed and line capacity is aptly answered with the creation of bandwidth rights and incorporation of such rights into the electronic distribution of content. In this way, specialist companies will strive through buying bandwidth of transmission capacity and adding value by attracting customers seeking said companies' accessible content.

20 Bandwidth rights are necessary as an improvement over the art. The INTERNET currently dominates any discussion of digital distribution. The INTERNET is built over lines or pipes. It is an important observation that a)

these pipes cost money to build, deploy and maintain, and b) the owners of the pipes must pay for their investment and earn some return, which is their motivation for building the infrastructure. The means by which files are transferred over the World Wide Web, the most mainstream segment of the

5 INTERNET, is the use and interpretation of Hypertext Mark-up Language (HTML) and embedded URLs (Uniform Resource Locators) which is designed to "alias" and designate a single path between the party that is viewing a reference of a file and the underlying file. The user is unnecessarily "connected" to the actual file, which is called "aliasing," and has effectively

10 created more network traffic and thus wasted bandwidth. This shortfall in HTML is affecting the INTERNET through inefficiencies resultant from the underlying connection-based TCP/IP protocol. In short, a lot of needless, bandwidth-wasting connections are continuously being created and destroyed. The current mechanics of the INTERNET will not be conducive to electronic

15 commerce, and must necessarily change. This fundamental aspect of splitting content from references to that content is amply addressed in U.S. Patent No. 5,428,606.

The biggest problem can be summed up by observing that users of the INTERNET generally live under the misconception that data or content is, or

20 should be, free. Although one can find specific instances of goods and services sold over the INTERNET, even downloadable software, the basic mechanism that underlies the sale is subject to this "fallacy of the free." There

5 unauthorized copies on an archive as disclosed in the digital watermark filings.

Recent legal actions against parties that distribute copyrighted music titles and game software has resulted in setting a "for price " trend that can be made more efficient by the present invention.

15 The present invention also presents improvements over exchanges that exist for the purpose of trading commodities such as stocks, bonds and other such securities. The distinctive feature of the preferred embodiment described below is the nature of the commodities being traded, bandwidth, and the unbounded potential of derivative copies of copyrighted works.

111589-1

present invention's improvements over the present art for both market exchange mechanisms and implementations of a content-based system that monitors copyrights and optimizes the distribution of the underlying content.

5 **The NASDAQ Market**

NASDAQ is an exchange that trades in a finite number of "titles" or stock certificates, whereas the present invention is concerned with the potential of an infinite number of "titles" made up of digital bits-- each derivative copy having the same potential commercial value as the original master copy that was intended for trade. The limited or finite commodity in question on a DICE exchange is available bandwidth for the actual transmission and thus delivery of a demanded, digitized "piece" of content (audio clip, picture, video, virtual reality, software, etc.). Bandwidth is characterized by the pipes that connect buyers and sellers of digital information and include POTs, cable, fiber optic, ISDN, satellite, electric power lines, etc. On the other hand, NASDAQ deals with basic stock securities, publicly-traded shares in companies. There are a small number of derivative securities traded, notably warrants, but the mechanisms for supporting a particular security are fairly uniform. NASDAQ is primarily an electronic bulletin board where market makers advertise at what prices they are willing to buy and sell a particular security. These market makers maintain an inventory of tradeable securities for sale to other parties, whether agency or principal-based transactions. A market maker does not

digital marketplace to increase activity and liquidity.

instance would be selling at 10 and buying at 9 7/8. Many market makers

trade the same stocks competitively, and in general, the more firms that make a market in a given stock, the more liquid the trading of that stock is, simply because there are more ready buyers and sellers. Again as a means to describe the present invention some understanding of these market

5 participants may be required in implementing the proposed system.

Although NASDAQ can be thought of as an "electronic" market, it is electronic, for the most part, only in the sense that instead of shouting across a floor at each other, traders generally advertise their price levels on a BBS (Bulletin Board System), which legally binds them to honor the price. They
10 then field phone calls from traders at other member firms, who have seen the advertisements on the BBS, and agree to trades over the phone. Then, each side enters their transaction (if one side is a BUY, the other is a SELL) into on-site computers, which all feed into central mainframes and link up with each other. Many errors are introduced by this process, and an error report is
15 produced at the end of the day, to be settled among the parties involved through after-hours reporting. So, there is really still a large low-tech component to NASDAQ which leads to discrepancies and inefficiencies.

The general public interacts with the market through brokers, who might also happen to work for a member firm. The chain of contact is individual to
20 broker to trader, with traders interacting among each other, and filling orders for brokers. This also touches the issues of primary and secondary markets. When a stock goes public, called an IPO (Initial Public Offering), shares are

bought up by a syndicate of market makers. This is the primary market. The proceeds of the IPO go to the issuing company, minus the underwriting fees, which are divided among the syndicate. The syndicate then sells shares to the public through brokers, and any other traders who want to trade them. The
5 syndicate may profit again by selling the shares at higher prices than the original purchase price. This trading continues indefinitely or until bankruptcy. This is the secondary market. Prices in the secondary market can vary continuously and widely from the price set in the primary market.

Having summarized the system, we can discuss some of the
10 inefficiencies and idiosyncrasies of NASDAQ to establish the parameters of the present invention in the preferred embodiment

One major problem is the uniform distribution of information. Theoretically, all traders should get the same information at the same time. However, NASDAQ does not accomplish this well. Since there are
15 intermediate "concentrators" between the terminals and the hub, and specific terminals tend to watch specific groups of stocks, some of which may be significantly more active than others, generating a larger volume of information per second, which can cause back-ups, in general, the system is plagued by delays of an intermittent and non-uniformly distributed nature. There is no
20 mechanism for detecting these problems, which may cause the display of old or incorrect prices for some stocks, and delay the dissemination of electronic orders on an unequal basis. Traders generally have several sources of

information, and need to be "on their feet", so the burden of detection is, in effect, placed on humans. NASDAQ terminals do maintain a "heartbeat." If the terminal cannot get a response from the hub for a prescribed period of time, a problem is signaled by turning the screen a uniform yellow on black.

Market makers have cooperated to run independent tests, and are well aware that one trader may see information up to several minutes before another.

A NASDAQ hub may send out information to all routes simultaneously, but there can be large delays before it arrives at the destination. An example of a timing performance protocol, which can be employed to counter such problems, is NTP (Network Time Protocol) on UNIX networks. NTP does advanced diagnosis of point-to-point network performance to forecast timing delays between pairs of machines. It is used with time critical applications, but not widely so, as it is still considered quite esoteric. NASDAQ makes no use of such protocols. For more trustworthy information about bandwidth rights and the aging of a media content good, the present invention takes into account forecasted timing delays for pricing the subsequent bandwidth right as an

7/11

overall component of the pricing of the media content being demanded, and delays in actually distributing this information. This is an improvement over the art as it is a more appropriate aspect of pricing media versus disseminating stock price information.

s at

}

ort

ve

Before considering the present invention's clearing operations, which are vital to simplifying the otherwise tremendous task of figuring out who owes what to whom at the end of the day, a description of the art, a la NASDAQ, is required. Basically, clearing is the matching up of trades. If one side reports a SELL, and the other a BUY, these two sides must be put together to form a trade which results in the transfer of money to the seller, and the transfer of the security to a buyer. Any halves of trades that do not match are kicked back to the member firm who entered them, for resolution. Provided the trade is resolved, both sides again enter their sides, only late. The securities can be held in street name, meaning the brokerage house can hold the physical shares for the buyer. However, the task of transferring stock certificates and cash among brokerage houses is onerous. Instead, a special holding organization was created. This organization is independent of the stock exchanges, but works with their clearing computers. The holding organization maintains vaults filled with stock certificates, held for the brokerage, which in turn hold the stock in the names of their clients. Everyone maintains records of who owns what relative to their own organization. Should an owner actually request their certificates, they can be removed from the vault and delivered by

I is

,

;

• Intrinsic Value

This value is measured versus a minimal standard telecommunications cost. If there is a single underlying telecommunications cost to the owner of the right of X dollars per minute, let min 0 represent the number of minutes it takes to download the information using the minimal bandwidth, and min 1 represent the number of minutes a to transfer the information at the bandwidth represented by this right. Note that $\text{min } 0 \geq \text{min } 1$.

Then the intrinsic value $VI = X \times (\text{min } 0 - \text{min } 1)$, or the amount of money saved in telecom costs at the higher bandwidth. The intrinsic value can be negative, which would imply a compensating premium placed on the time saved by using the more expensive transport.

• Percentage Chance of Failure

This probability recognizes the generally unreliable nature of the current telecommunications and transmission mediums as well as underlying computer systems. Rather than be burdened with the task of solving all of the "bugs" in a given piece of commercial software, it would be better to account for failure in the valuation. This value could be adjusted over time, as the failure probability of a system becomes more apparent, or changes. In short, this represents the percentage chance a user cannot exercise their right. It affects the expected value of the right. In this baseline approach, if the probability of failure is P_f ,

- Convenience Premium

$$V_{\text{real}} = V_{\text{theoretical}} + V_C$$

This is a function of the exercise period of the bandwidth right. It is proportional to P_f , since more time allows for recovery from an individual failure to transfer. There are two components of time, over what period a transfer can be initiated and for how long the transfer can last once it is initiated. Note that this is made more complex by congestion factors. For instance, if a user has a right for 10,000 kbps for 10 seconds, and the user wants to transfer 100,000 kb, it is not likely that the transfer can be done in exactly 10 seconds. Protocol

overhead and congestion will add some increment of time. It is advisable to leave room in the exercise period for these factors, rather than trying to value the time value in some manner which accounts for these transient conditions.

Thus:

$$V = (1 - Pf)(V_I + V_T + V_C)$$

$$\text{or } V = (1 - Pf) ((X(\min 0 - \min 1) + V_T) + V_C$$

The convenience premium, V_C , should be independent of all other values (except V).

The equation behaves as such:

With increased failure probability decreasing rights value, independent of other variables, while increased demand relative to supply would drive up V_C . We might try to compute V_C by accounting for known demand and supply values, and in fact, it is of vital importance to know the supply, and to allocate it so that any right issued can be exercised within its exercise period.

Additionally, it is observed that a method is needed to allocate supply based on demand which accounts for unused rights. In other words, the system needs to over allocate supply to some degree, knowing that some rights may go unexercised, so that demand is filled as much as possible. This is similar to airlines' practice of overbooking flights.

Some mechanism must be in place to prevent attacks on the system, by a party, who, in effect, tries to corner the market in bandwidth, with no intention

of using it, so that it goes unused. Naively, one would think that since one has to pay for the bandwidth, why would someone want to corner the market?

Although bandwidth is not free, it should only comprise a small fraction of the value of the information to be transferred, and so this is not an unthinkable

5 situation. The likeliest preventive measure is the existence of competition in transmission.

Another option is the potential need to necessitate a secondary market for the trading of bandwidth, which could be divided up by a trading syndicate, and traded on a secondary basis to users. In a manner of operations,

10 telecommunications companies perform this role between national telecommunications systems to facilitate international phone usage. But the difference with the system envisioned in the present system is that "any" user could buy bandwidth rights at times of low demand, and hope to sell them at a profit in times of higher demand. This would seem to imply the exchange itself

15 should do some proprietary trading in this manner, both to profit, and to ensure some bandwidth is available for sale to users when they need it. This will have a purpose to serve in making the market efficient in the future.

Bandwidth rights instruments are likely to be highly localized to specific subnets. Especially since certain types of connections may be available only

20 from certain exchanges, and since failure probabilities are likely to vary with specific hardware, operating systems, and service providers. Additionally, the basic valuation equations above do not address telecommunications costs

across various types of lines. This problem at least, might be solved by active maintenance of cost tables, designation codes for types of lines, and the designation of a low cost standard. The problem of moving rights between exchanges is made more difficult since supply/demand planning for one exchange will not translate to another, unless some means for interconnecting exchanges is developed, and exchange bandwidth planning is global. The race by many parties to link users to the INTERNET via varying access links (modem) including ISDN, POTs, cable, may further the need for common bandwidth pricing. What is clear is that the basic structure of the present invention would facilitate such planning to the benefit of all market participants: telecoms providers, INTERNET access companies, users and publishers as well as more general aggregators of content and bandwidth such as, phone companies, cable companies and satellite companies intending on providing services across multifarious line types.

Bandwidth Rights Accounting and Clearing

If a bandwidth right is securitized, the creation and supply of certificates, made unique by cryptographic methods to manage them, will also be necessary. Transferring certificates between individuals is complicated and unnecessary. Following the general principles of the securities clearing model described above seems to be in order. In this case, the exchange needs to create and manage an account for each party that can own or trade bandwidth

rights. Additionally, a method for authenticating the party is required. With these two elements, a trading market can be implemented by the following methods:

5 The exchange creates and manages a supply of uniquely distinguished bandwidth rights certificates. These certificates are good for a specific period only. They may be traded over the course of time, anywhere from the moment they are created to the expiration time. It is questionable whether a right should be exercisable once it is clear that even if a transfer is initiated, it cannot be completed given that right only. However, consider that the right is
10 usable, but its value decreases rapidly as it approaches expiration (i.e. value is based on time left, not total transfer time). Once a certificate is expired it is deleted. Hash values incorporating a time-stamp could be used to serialize certificates. Such a cryptographic method is well noted in the art. US Pat No 5,136,646 and 5,136,647 ("Digital Document Time-Stamping With Catenate
15 Certificate" and "Method For Secure Time-Stamping Of Digital Documents" respectively) describe methods for cryptographic time-stamping.

The exchange creates a central hub for planning bandwidth supply, accounting, and disseminating pricing information. Client-side software will value the rights relative to a particular user's needs, and used by any party
20 trading rights. A seller creates a SELL advertisement, which is entered into the "exchange". The exchange verifies that the seller actually holds the right in their account. A buyer then enters a BUY offer against the sell advertisement.

5

10

15

through party B, to party C, then:

5 The above example should make clear the relationships between
upstream and downstream parties.

A significant improvement over traditional metering systems is that exchange mechanisms are beneficially tied into content for more realistic metering of playing or recording content. With multichannel digital watermarks, a more robust means for metering content is made possible by parties not willing to create expensive proprietary distribution channels, but who do wish to capitalize on selling content in the economic method of metering. There are two immediately apparent schemes which might accomplish this. The first is described as a "passive" scheme and the second is described as an "active" scheme.

002010:000400

In a passive scheme, several assumptions must be decided and jointly agreed upon beforehand by all parties who wish to add watermarks. Based upon the total number of watermark channels to be used, where each party that wants to add a watermark is assumed to use at least one watermark

5 channel, and the amount of data, and the desired minimal level of watermark security, a watermark system could encode watermarks at an appropriate sparsity such that random chance will cause some watermarks added by downstream parties to obliterate watermarks added by upstream parties. But by the same token, random chance will allow some of the watermarks of

10 upstream parties to survive the encoding of watermarks by downstream parties by virtue of the fact that such watermarks do not occupy enough of the same data space to cause one to significantly interfere with the reading of another. The end result is that at least one watermark added by each party will be readable at the final destination. While such a passive scheme is appealing

15 because of its relative simplicity, in which each party can add watermarks without considering the impact of any other party, once some initial parameters are set, this type of scheme requires a lot of testing to determine optimal settings given various initial conditions, and does not guarantee any particular level of watermark redundancy. It is quite haphazard, although technically

20 feasible.

According to an advantageous embodiment of the present invention, an

active scheme is implemented which is described as follows. The farthest party upstream, who presumably controls the ultimate copyrights and distribution rights of the data generates two keys. The first key is a regular watermark key, as described in previous related patent application disclosures by The DICE Company, particularly, including the "Method for Stega-Cipher Protection of Computer Code" application. This key is used for actual encoding and decoding of information from the watermark channel "owned" by this party. The second key is a new type of watermark key, called a master framework key, which dictates

- 10 how the entire data stream in general is to be packetized;
- how the data stream packets are to be allocated among a
- predetermined number of reserved watermark channels; and
- how the channels are to be assigned to downstream parties.

This information is the minimal amount of information which must be shared with downstream parties to enable them to add watermarks using their own regular watermark keys to their assigned channels. Notice that within a given channel, another key is still needed to extract a watermark. Therefore, while some information is potentially leaked, the watermarks are still secure. The master framework key, in effect, creates several virtual data streams within the real data stream, each of which can be accessed separately by the watermark system. The master framework key can then be shared on a limited or protected basis with only those downstream parties who the upstream party

chooses to participate in the distribution. Such master keys could be distributed using well-known cryptographic art for key transmission. Each downstream party is responsible for generating their own regular watermark key, and watermarking their assigned channel with appropriately generated information using the combination of the master framework key and the regular watermark key, as the data is received and forwarded. This active scheme is much better than the passive scheme, since it ensures that watermarks added by downstream parties do not interfere in any way with those added by upstream parties, thus guaranteeing a maximal level of watermark redundancy, which is desirable, while minimizing the disclosure of watermark information necessary to downstream parties, which is undesirable. It is envisioned that systems that use a hybrid approach, incorporating some mechanisms and methods of the active scheme, but also relying on some methods of the passive scheme may be developed.

15

Keysearch Optimization Mechanisms and Techniques

Another issue of digital watermark system which must be adequately addressed is key search. When a suspect copy of content is obtained, the amount of work done to extract watermark information from the copy is bounded by the set of watermark keys which are potential candidates which may have been used to encode the hypothetical watermark(s) in the suspect data. It is an object of the invention described herein to minimize the amount of

work and hence time required to search this set of keys, or keyspace, while ensuring confidence that all potential candidate keys have been searched, or at least those candidates with a significant probability of constituting the actual target of the search.

5

The watermark decode operation proceeds generally as follows: First a candidate key search group is generated, then a decode process is run using each candidate key until either all keys are exhausted and no watermark is extracted, or a watermark is extracted using a candidate key. Depending on the nature of the information in the extracted watermark, the search might continue with remaining keys, or terminate. One obvious method for improvement is to perform parallel searches trying multiple keys at the same time. Using powerful parallel hardware, real gains may be obtained using this method simply.

On slower, serial CPU-based hardware, real parallel gains are more difficult to make. However, using dynamic programming techniques and intelligent search scoring and management, one could configure the search engine to start with several or all keys, checking each packet of data against each key before proceeding. As each iteration is completed, factoring in the next data packet, cumulative "scores" for the results of each key may be computed and compared. Keys which appear to have more potential to ultimately yield a match and extract a watermark continue to be used in the

process, while those with lower potential, as measured by score, are dropped from the process. This process has an attractive characteristic that it gets faster as more keys are progressively eliminated from the search space, and can consider a large number of keys. Its drawback, in the absence of other

5 techniques, is that the initial key space may be very large, and it may take considerable time to narrow the search keys to the point where the search proceeds at a reasonably fast pace. It is also possible that the process of finding a match does not score in a monotonically increasing manner, resulting in the early elimination of the correct key. In other words, scores may get worse

10 before they get better.

Without considering any information about the source copy used to generate the suspect copy, one could limit the search work done by imposing a limit on how much time a decoder can spend checking data versus a particular key, or a maximal percentage, or number of packets of the copy to process

15 before giving up on a given key. One could do well with a heuristic rule that says, "if I have checked 50% of the recording without finding a watermark, then in all likelihood I will not find a watermark in the other 50% of the recording with this particular key," for instance. However, the best gains can be made by eliminating as many keys as possible from the initial search pool. In order to

20 do this the keys are expanded to include several items of information regarding the source copy or master that was watermarked using the key in question. This information includes any of the following items:

Title, Artist, Date, size of recording, format of the recording, quality of the recording;

and may also include mathematically calculated properties of the recording which can identify the recording to some significant degree of probability while using only a small amount of data (i.e. localized hash values, etc.). When a suspect copy is obtained, this same set of information describing the suspect copy is generated by the decoder system, which can then select a set of candidate keys which match to a desired degree, any or all the criteria stored with the keys.

10

Finally, the best potential results may be obtained by taking advantage of the multiple access levels made possible by the watermark system described in previous filings. A watermark embedded in a higher privacy channel corresponds with a particular key. Every key has a unique identification which allows the key custodian to find the key in a database, but provides no information on the key itself. This identification may have no meaning outside the custodial system. If the higher privacy key identification is included in a lower privacy watermark such as a protected or public watermark, then the party searching for the higher privacy watermark makes use of an intentionally limited set of lower privacy keys to first extract the key identification of the higher privacy key. At this point, no additional key search is necessary, thus allowing significant time savings. This assumes the lower

privacy watermark has not somehow been removed from the digital sample stream.

An embodiment of the decoder key search system encodes private key identifiers in lower privacy watermarks and uses descriptive information in the
 5 keys to compare versus the suspect copy to narrow the key search space.

This embodiment makes use of parallel hardware to facilitate as much gain as possible from parallel search techniques described above, including progressive elimination of keys which appear to diverge from a match as the comparison progresses.

10 In an exchange mechanism according to an embodiment of the present invention, the exchange is not the source of any of the sought-after works or digital information packages (DIPs). The exchange is ultimately measured by available transmission resources. Whereas DIPs are measured in a digitization system, the size of the underlying data file, its file structure, which dictates any
 15 potential compression and buffering, and data overhead for error correction, will provide exchange participants with an estimate for the resources, including time required to distribute said DIP. Given the heterogeneous nature of existing and proposed line infrastructure, any DIP can potentially be
 20 exchanged over vastly different lines between points. These may include copper, coaxial, fiber optic, etc. Distribution of a given DIP may occur on different lines for the same work (say for instances of a work available over POTs and satellite, etc.) or over a number of different media in the distribution

002040 5854960

of a work as it is transmitted over a network with a plurality of transmission media (say, the backbone of the network may be fiber but the end loop is coax, etc.). Given the existence of other traffic over these lines, including telephony, the pricing of a given DIP should necessarily include the price of the bandwidth resources necessary to transfer the DIP between at least two parties. As previously discussed, the difference in this embodiment and systems such as video-on-demand or proprietary cable and satellite systems is the necessity to value bandwidth between points in a network to facilitate the exchange of a demanded work at a given instant in time not continuously as with traditional "subscriber models." Similarly, "time-share" systems are oriented around selling a parcel of time to users seeking "processor" access to perform some activity, while, bandwidth is not the commodity being bid, time shares are reservation systems not capable of bidirectional or end-to-end "negotiation" of resources to facilitate the exchange of a DIP in real or next-to-real time.

Further, the preferred embodiment differs in that all participants may have significantly different access infrastructure (differing modems, cable, electric powerline, satellite, etc.) and pricing preferences given demand for a particular DIP.

The price of the bandwidth resources is, thus, proportional to the percentage of bandwidth allocated to the transfer of the DIP and inversely proportional to the duration of the transfer. With these factors, the aggregate of available bandwidth must change with time and can appropriately be priced

given the demand of certain DIPs or publishers seeking to effectively distribute DIPs. Bandwidth allocation can then be securitized to reflect the varying needs of market participants to exchange DIPs. How this security is priced relates to the nature of the underlying DIP which is most likely a luxury item such as a musical recording or video game. The securities must then trade independently of the DIPs and are based in part on a convenience premium, given demand for bandwidth allocation at any given time. Additionally, network resources as measured by present digital packet switches provide the variable of "supply of bandwidth resources" and estimated demand for said resources at a given time. For networks that are more centralized, such as cable or satellite, estimating bandwidth resources may actually be far easier as traffic is generally downstream to customers not bidirectional like telephone networks. Further means for computing bandwidth securitization instruments take into consideration probability of failure to exercise an instrument, the time period for which said instrument is valid, intrinsic value relative to minimum standard bandwidth utilization for the line in question. These factors, when coupled with a convenience premium, are improvements over the prior art as described in the U.S. Patent No. 5,428,606. Bidirectional exchange of content by parties who can be both subscribers or publishers or both, are possible when the party wishing to sell content or DIPs can set distribution, pricing, and other informational fields at its discretion. These issues are well documented in U.S. Patent No. 5,428,606 and are increasingly important in the growing popularity

of the World Wide Web (WWW) portion of the INTERNET. But, given that the marketplace in which digital goods can be traded digitally is itself digital, the evident or potential scarcity of bandwidth or the ability to value existing bandwidth given a commercial market for digital goods exchange is invaluable.

5 Further, security of the content and records of said content can be further described as an improvement over methods to undeniably identify content through the use of digital watermarks and other similar technologies. It is desirable to take appropriate measures to protect as many parties as possible in the transaction of a copyrighted work. These parties may include
10 the copyright holder, publisher, distributor, retailer, and consumer. As with the physical monitoring of media products such as CDs, where physical checks are conducted by the label, manufacturer, distributor, retailer and even outside parties such as SoundScan, Billboard, etc. the digital domain contains far less means for "hands-on" metering without including watermarks as "secured
15 identification" for parties involved in the distribution chain. As a preferred embodiment of the present invention, a record of a given DIP should include at least two of any of the following three elements: a digital watermark key, a DIP header, and a bandwidth securitization instrument (bandwidth right). The DIP header describes the content, its address, pricing, and distribution. The
20 bandwidth right is unique in its instance but also varies according to network bandwidth availability for a given period of time and the duration of the actual use of bandwidth on said network.

002040, 6994360

Optimizing key searches and increased use of multichannel digital watermarks are delineated in the discussions that follow this preferred embodiment as they are additional improvements over the art. The embodiment thus far discussed makes possible a more "democratically" or

5 "economically" feasible market for the exchange of digital goods. With bandwidth rights, multichannel watermarking, optimized key searches, content-base metering, it will be possible to more fully replicate retail and wholesale environments as they exist in the physical world. Decisions about depth and breadth of services and goods that can be offered by on-line market

10 participants will differ only in the ability to offer access to archives (POTs, cable, satellite, wireless, etc.) which will be determined by pricing and speed of transmission as well as by content providers interested in tapping into the potential distribution market that the pipe owner's network includes. Market participants will also be able to appeal to the anonymous parties that seek

15 content through attractiveness of a "site, " amount of processing speed available for distributing digital goods, staff responsible for purchasing or creating available content for downloads, the number of available repurchase rights of copyrighted works: "electronic window-shopping" can be realized given heterogeneous networks, many digital goods, and the creation of

20 bandwidth rights to complement digital watermarking systems. Simply, content can better be valued given the infrastructure of the digital domain while recognizing/he importance of tracking and monitoring the exchange of digital

